

日 本 国 特 許 庁

PATENT OFFICE  
JAPANESE GOVERNMENT

JC808 U.S. PTO  
09/619699  
07/19/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2 0 0 0 年 2 月 2 4 日

出 願 番 号

Application Number:

特 願 2 0 0 0 - 0 4 7 3 2 3

出 願 人

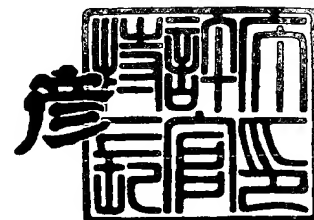
Applicant (s):

日本電信電話株式会社

2 0 0 0 年 6 月 2 3 日

特 許 庁 長 官  
Commissioner,  
Patent Office

近 藤 隆 彦



出 証 番 号 出 証 特 2 0 0 0 - 3 0 4 6 8 3 8

【書類名】 特許願

【整理番号】 NTTH116889

【提出日】 平成12年 2月24日

【あて先】 特許庁長官殿

【国際特許分類】 G09C

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

【氏名】 小林 邦生

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

【氏名】 森田 光

【特許出願人】

【識別番号】 000004226

【氏名又は名称】 日本電信電話株式会社

【代理人】

【識別番号】 100066153

【弁理士】

【氏名又は名称】 草野 卓

【選任した代理人】

【識別番号】 100100642

【弁理士】

【氏名又は名称】 稲垣 稔

【手数料の表示】

【予納台帳番号】 002897

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9806848

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 大小比較方法、その装置及びプログラム記録媒体

【特許請求の範囲】

【請求項 1】 参加者  $j$  は  $N$  種の指標値  $1, 2, \dots, N$  から選んだ意中の指標値  $i_j$  と、初期値  $IV_j$  と、 $1$  以上の任意の整数  $x_j$  を参加者装置に入力し、

参加者装置は  $IV_j$  に一方向性関数  $g$  を  $x_j$  回施し、その値  $g^{x_j}(IV_j)$  に対し、 $g$  と異なる一方向性関数  $h$  を  $N - i_j$  回施し、その値  $A_j = h^{N-i_j}(g^{x_j}(IV_j))$  を中央装置へ送って意中の指標値  $i_j$  を間接的に登録し、

中央装置は全参加者装置から  $A_j$  を受信後に、 $k = N, N - 1, N - 2, \dots$  と順次、 $k$  で登録したかどうかの問合せを各参加者装置へ送信し、

各参加者装置は受信した問合せ  $k$  が自分の意中の指標値とは異なる場合は  $B_{k,j} = h^{k-i_j-1}(g^{x_j}(IV_j))$  を中央装置へ送信し、

中央装置は受信した  $B_{k,j}$  に一方向性関数  $h$  を施し、 $h(B_{k,j}) = A_j$  となることを検証し、 $A_j$  の値を受信した  $B_{k,j}$  に変更し、

自分の意中の指標値と問合せの  $k$  が同一である参加者  $j$  の装置は  $B_{k,j} = g^{x_j-1}(IV_j)$  を中央装置へ送り、

中央装置は受信した  $B_{k,j}$  に一方向性関数  $g$  を施し、 $g(B_{k,j}) = A_j$  となることを検証し、

自分の意中の指標値が  $k$  で上記順次の問合せに対し、初めてある参加者  $j$  の意中の指標値が  $k$  と同一であることが検証されたとき、その指標値  $k$  を全参加者の意中値のうちの最大値として出力することを特徴とする大小比較方法。

【請求項 2】 請求項 1 記載の方法において、

自分の意中の指標と問合せの  $k$  が同一である参加者  $j$  の装置は同一であることを示す同一情報も中央装置へ送り、

中央装置は参加者装置からの受信情報中に同一情報が含まれていない場合は、上記  $h(B_{k,j}) = A_j$  かの検証を行い、同一情報が含まれている場合は上記  $g(B_{k,j}) = A_j$  の検証を行うことを特徴とする大小比較方法。

【請求項 3】 請求項 1 記載の方法において、

中央装置は上記  $h(B_{k,j}) = A_j$  の検証において不一致の場合は上記  $g(B_{k,j}) = A_j$  の検証を行うことを特徴とする大小比較方法。

$j$ ) =  $A_j$  の検証を行うことを特徴とする大小比較方法。

【請求項 4】 請求項 1 乃至 3 の何れかに記載の方法において、

上記  $N$  種の指標値  $1, 2, \dots, N$  は  $N$  個の値  $P_1, P_2, \dots, P_N$  とその大小順に対応付けられてあり、

参加者は  $P_1, P_2, \dots, P_N$  から選んだ意中の 1 つを参加者装置に入力することにより上記指標値  $i_j$  の入力を行い、

上記全参加者の意中指標値のうちの最大値  $k$  と対応する値  $P_k$  を最大値又は最小値として出力することを特徴とする大小比較方法。

【請求項 5】  $N$  種の指標値  $1, 2, \dots, N$  から選んだ 1 つの指標値  $i_j$ 、初期値  $IV_j$ 、1 以上の任意の整数値  $x_j$  を入力する入力手段と、

入力値に対し、一方向性関数  $g$  を施す  $g$  演算手段と、

入力値に対し、一方向性関数  $h$  を施す  $h$  演算手段と、

記憶手段と、

中央装置と情報の送受信を行う送受信手段と、

指標値  $i_j$ 、初期値  $IV_j$ 、整数値  $x_j$  を記憶手段に記憶し、 $A_j = h^{N-i_j} (g^{x_j} (IV_j))$  を生成して中央装置へ送り、中央装置から  $k$  登録かの問合せを受信すると、 $k \neq i_j$  であれば  $B_{k,j} = h^{k-i_j-1} (g^{x_j} (IV_j))$  を生成し、 $k = i_j$  であれば、 $B_{k,j} = g^{x_j-1} (IV_j)$  を生成して  $B_{k,j}$  を中央装置へ送信する制御手段と、

を具備する参加者装置。

【請求項 6】 請求項 5 記載の装置において、

$P_1, P_2, \dots, P_N$  なる値をその大小順に上記指標値  $1, 2, \dots, N$  を対応付けた換算テーブルを備え、

上記入力手段に指標値  $i_j$  に代え、 $P_1, P_2, \dots, P_N$  から選んだ 1 つの値  $P_{k,j}$  が入力され、

上記制御手段は、入力された値  $P_j$  を上記換算テーブルを参照して指標値  $i_j$  に変換することを特徴とする参加者装置。

【請求項 7】 複数の参加者装置から間接的に登録された意中の指標値の大小関係を比較する装置であって、

記憶手段と、

入力値に対し、一方向性関数  $g$  を施す  $g$  演算手段と、

入力値に対し、一方向性関数  $h$  を施す  $h$  演算手段と、

各値  $k$  から 1 つずつ減算する減算手段と、

各参加者装置と情報の送受信を行う送受信手段と、

各参加者装置からの登録情報  $A_j$  を記憶手段に記憶し、全参加者装置からの登録情報  $A_j$  の受信後に、上記値  $k$  を指標値の最大値  $N$  に設定し、各参加者装置に値  $k$  で登録を行ったかの問合せを送り、その応答情報  $B_{k,j}$  に対し一方向性関数  $h$  を施し、その値  $h(B_{k,j})$  が対応する  $A_j$  と等しいことを確認し、その  $A_j$  の値を受信した  $B_{k,j}$  の値に変更し、全参加者装置からの応答情報を処理すると  $k$  を  $-1$  して問合せをすることを繰返し、登録した意中の指標値と問合せの  $k$  が同一である参加者装置の応答情報  $B_{k,j}$  に対し、一方向性関数  $g$  を施し、その値  $g(B_{k,j})$  が対応する  $A_j$  と等しいことを確認して、その  $k$  が全登録指標値中の最大値として出力する制御手段と

を具備する中央装置。

【請求項 8】 請求項 7 記載の装置において、

$N$  種の指標値  $1, 2, \dots, N$  に対し、 $N$  個の値  $P_1, P_2, \dots, P_N$  をその大小順に対応付けた換算テーブルを備え、

制御手段は上記最大値とした指標値  $k$  と対応する値  $P_k$  を換算テーブルを参照して、全登録値中の最大値又は最小値として出力することを特徴とする中央装置

【請求項 9】 参加者装置から、 $N$  種の指標値  $1, 2, \dots, N$  から選んだ 1 つの指標値  $i_j$  を中央装置に間接的に登録し、中央装置で全登録指標値中の最大値を求めシステムにおける参加者装置のコンピュータに、

入力された指標値  $i_j$ 、初期値  $IV_j$ 、1 以上の任意の整数  $x_j$  を記憶手段に記憶する処理と、

$IV_j$  に対し一方向性関数  $g$  を  $x_j$  回施して  $g^{x_j}(IV_j)$  を得る処理と、

$g^{x_j}(IV_j)$  に対し、一方向性関数  $h$  を  $N - i_j$  回施して  $A_j = h^{N-i_j}(g^{x_j}(IV_j))$  を得る処理と、

$A_j$ を中央装置へ送信する処理と、

中央装置から  $k$  で登録したかの問合せを受信する処理と、

$k = i_j$  でなければ  $B_{k,j} = h^{k-i_j-1} (g^{x_j} (I V_j))$  を演算する処理と、

$k = i_j$  であれば  $B_{k,j} = g^{x_i-1} (I V_j)$  を演算する処理と、

$B_{k,j}$ を中央装置へ送信する処理と

を実行させるプログラムを記録した記録媒体。

【請求項 1 0】 請求項 9 記載の記録媒体において、

入力された値  $P_j$  を、指標値  $1, 2, \dots, N$  に対し、値  $P_1, P_2, \dots, P_N$  が大小順に対応付けられた換算テーブルを参照して  $i_j$  に変換して、 $i_j$  を入力する処理を

上記コンピュータに実行させるプログラムを上記プログラムが含むことを特徴とする記録媒体。

【請求項 1 1】 複数の参加者装置から、 $N$  種の指標値  $1, 2, \dots, N$  から選んだ 1 つの指標値  $i_j$  を登録情報  $A_j$  によりそれぞれ中央装置に間接的に登録し、中央装置で全登録指標値中の最大値を求める中央装置のコンピュータに、

各参加者装置からの登録情報  $A_j$  を受信する処理と、

受信した登録情報  $A_j$  を記憶手段に記憶する処理と、

全参加者装置からの登録情報  $A_j$  を受信した後に、値  $k$  に  $N$  を設定して  $k$  で登録したかの問合せを各参加者装置へ送信する処理と、

問合せに対する応答情報  $B_{k,j}$  を受信する処理と、

$k$  に対する登録をしてない参加者装置からの  $B_{k,j}$  に対し一方向性関数  $h$  を施し  $h(B_{k,j})$  を求める処理と、

受信  $B_{k,j}$  と対する  $A_j$  を記憶手段から読出して、 $h(B_{k,j}) = A_j$  であるかを検証する処理と、

$h(B_{k,j}) = A_j$  であれば、 $A_j$  として  $B_{k,j}$  を記憶手段に記憶する処理と、

全参加者装置から応答情報を受信すると、 $k$  を 1 減算して上記問合せ処理以下を繰返す処理と、

$k$  に対する登録をしている参加者装置からの  $B_{k,j}$  に対し、一方向性関数  $g$  を施して  $g(B_{k,j})$  を求める処理と、

$B_{k,j}$ と対応する $A_j$ を記憶手段から読出して $g(B_{k,j}) = A_j$ であるかを検証する処理と、

その検証に合格すると、その $k$ を全登録指標値の最大値として出力する処理とを実行させるプログラムを記録した記録媒体。

【請求項 1 2】 請求項 1 1 記載の記録媒体において、

上記最大値とした $k$ により、指標値 1, 2, ...,  $N$ に対し、値 $P_1, P_2, \dots, P_N$ が大小順に対応付けられた換算テーブルを参照して値 $P_k$ を最大値又は最小値として出力する処理を上記コンピュータに実行させるプログラムを上記プログラムが含むことを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は情報セキュリティ技術の応用技術に関するものであり、特にインターネットなどにより多数の参加者がオンラインでアクセス可能な状況下で、各々の秘密値の大小を比較する方法に関するものであり、電子くじ、電子投票、電子入札など様々なアプリケーション（応用分野）での利用が可能である。

【0002】

【従来の技術】

例えば電子競争入札は図 7 に示す様に、参加者毎に設けられる参加者装置、この場合は入札装置 1 1<sub>1</sub>, 1 1<sub>2</sub>, ..., 1 1<sub>M</sub>と、これらと例えばネットワークで接続され、全体を統合的に処理する中央装置、この場合は開票装置 1 2 から構成され、各 1, 2, 3, ...,  $N$ の $N$ 種の指標値に対応して、初期値 $IV$ に一方向性関数 $h$ を多重に施し、つまり $IV$ に $i$ 回の一方向性関数を施す場合、 $h^i(IV)$ と表現し、これは $h(h(h(\dots h(IV)\dots)))$ （この $h$ の数は $i$ ）を意味する。これら $h(IV)$ ,  $h^2(IV)$ ,  $h^3(IV)$ , ...,  $h^N(IV)$ なる値をそれぞれ指標値 1, 2, 3, ...,  $N$ と対応させることとし、各参加者 $j$  ( $j = 1, 2, \dots, M$ ) はその入札装置 1 1<sub>j</sub>から $A_j = (h^{N+1}(IV_j), g(h^{ij}(IV_j)))$ なる一対の値を生成して、開票装置 1 2 に送ることで、その参加者 $j$ の意中の指標値（秘密値） $i_j$ を間接的に登録する。 $g(A)$ は $A$ に一方向



性関数  $g$  を施すことを表わし、またその明細書では  $i_j$  を添字として用いる場合は例えば「 $i_j$ 」と表記する。開票装置 12 は全参加者からの登録を受信した後、カウンタ 13 を初期値  $N$  から順次ダウンカウントし、そのカウンタ 13 の各値  $k$  ( $N, N-1, \dots, 1$ ) について登録した参加者  $j$  がいるかどうかを、全参加者端末装置  $11_1, \dots, 11_M$  に順次  $k$  を送信して尋ね、各入札装置  $11_j$  は該当しないときは、 $B_{k,j} = h^k (IV_j)$  を開票装置 12 へ応答し、開票装置 12 は  $h(B_{k,j}) = A_j$  および  $g(B_{k,j}) \neq C_j$  となることを確認して、その参加者  $j$  の意中の指標値が  $k$  ではないということを証明し、 $A_j$  の値を受信した  $B_{k,j}$  に変更して次の  $k$  に備え、

問合せに対し自分の意中の指標値と  $k$  が同一である参加者  $j$  は  $B_{k,j} = h^k (IV_j)$  を開票装置 12 へ送り、開票装置 12 は受信した  $B_{k,j}$  に対し、 $h(B_{k,j}) = A_j$  および  $g(B_{k,j}) = C_j$  となることを確認して、その参加者  $j$  の意中の指標値が  $k$  であることを証明する。

#### 【0003】

初めてある参加者の意中の指標値が  $k$  であるものが現われ、かつこれが証明されたとき、その  $k$  を登録した全指標値中の最大値であることとする。

#### 【0004】

##### 【発明が解決しようとする課題】

従来の方法ではその値の正当性を検証するために、1 指標値、1 参加者ごとに

$$h(B_{k,j}) = A_j$$

$$g(B_{k,j}) = C_j$$

と 2 つの式が成立するかの検証が必要であり、指標値数と参加者数の増大により、その処理量が膨大なものとなる欠点があった。

#### 【0005】

##### 【課題を解決するための手段】

この発明によれば一方向性関数を利用して、秘密値を  $h^{N-i_j} (g^{x_j} (IV_j))$  に変換して登録する。 $x_j$  は参加者が決める 1 以上の任意の整数である。また参加者は  $k$  で登録したかの問合せに対し、意中の秘密値でなければ  $B_{k,j} = h^{k-i_j-1} (g^{x_j} (IV_j))$  を提示し、意中の秘密値であれば  $B_{k,j} = g^{x_i-1} (IV_j)$

を提示し、中央装置は前者に対しては  $h(B_{k,j}) = A_j$  により、後者に対しては  $g(B_{k,j}) = A_j$  により検証する。

【0006】

【発明の実施の形態】

図1にこの発明の実施例を示す。複数の参加者  $j$  ( $1, 2, \dots, M$ ) の装置 (図には1つのみを示してあるが複数設けられている)  $11_j$  は中央装置  $12$  へ指標値  $i_j$  を間接的に登録し、中央装置  $12$  でその登録された指標値  $i_j$  中の最大値を求める。参加者装置  $11_j$  は例えば入札装置、中央装置  $12$  は例えば開票装置である。  $N$  種の指標値  $1, 2, \dots, N$  に対し、  $N$  個の値  $P_1, P_2, \dots, P_N$  が大小順に対応付けられた換算テーブル  $21$  が各入札装置  $11_j$  と開票装置  $12$  に設けられる。図1の例は  $P_1 = 10, P_2 = 15, P_3 = 30, \dots, P_N = 3000$  と指標値  $k$  ( $1, 2, \dots, N$ ) が大きくなるに従って値  $P_k$  が大きくなるように対応付けた場合である。

【0007】

図2に入札装置  $11_j$  の機能構成を示し、図3にその処理手順を示す。参加者  $j$  は入力手段  $22$  により、  $N$  個の値  $P_1, P_2, \dots, P_N$  から1つ選んだ値  $P_j$  と、初期値 (正整数)  $IV_j$  と、1以上の任意の整数  $x_j$  を入力する (S1)。制御部  $23$  は  $IV_j, x_j$  を記憶部  $24$  に記憶する (S2) と共に  $P_j$  により換算テーブル  $21$  を参照して  $P_j$  を指標値  $i_j$  に変換して記憶部  $24$  に記憶する (S3)。

次に  $IV_j$  と  $x_j$  を取出して  $g$  演算部  $25$  に入力して、  $IV_j$  に対し、一方向性関数  $g$  を  $x_j$  回施して  $g^{x_j}(IV_j)$  を求め (S4)、必要に応じてこれを記憶部  $24$  に記憶する (S5)。次にこの  $g^{x_j}(IV_j)$ 、  $N$ 、  $i_j$  を  $h$  演算部  $26$  に入力して、  $g^{x_j}(IV_j)$  に対し、一方向性関数  $h$  を  $N - i_j$  回施して、

$$A_j = h^{N-i_j}(g^{x_j}(IV_j))$$

を求め (S6)、送受信部  $27$  へ登録情報として  $A_j$  を開票装置  $12$  へ送信する (S7)。このようにして参加者  $j$  は意中の指標値  $i_j$  を開票装置  $12$  に間接的に登録する。

【0008】

開票装置  $12$  の機能構成を図5に、処理手順を図6にそれぞれ示す。開票装置

1 2 は送受信部 3 1 に各参加者装置 1 1<sub>j</sub>からの登録情報  $A_j$  が受信されると、制御部 3 2 はその  $A_j$  を記憶部 3 3 に記憶する (S 1)。全参加者装置 1 1<sub>j</sub>からの登録情報  $A_j$  が受信されると (S 2)、カウンタ 1 3 に初期値  $N$  を設定し (S 3)、カウンタ 1 3 の計数值  $k$  で登録したかの問合せを送受信部 3 1 を通じて各参加者装置 1 1<sub>j</sub> に送信する (S 4)。

【0 0 0 9】

各参加者装置 1 1<sub>j</sub> は図 3 に示すように開票装置 1 2 からの問合せを送受信部 2 7 で受信すると (S 8)、その問合せ指標値  $k$  が記憶部 2 4 内の  $i_j$  と等しいかを調べ (S 9)、等しくなければつまり  $k$  がその参加者の意中の指標値  $i_j$  でなければ、記憶部 2 4 から  $g^{x_j} (I V_j)$  を取り出し、これと  $i_j$ ,  $k$  を  $h$  演算部 2 6 に入力して  $g^{x_j} (I V_j)$  に対し一方向性関数  $h$  を  $k - i_j$  回施して応答情報  $B_{k,j}$  を求める (S 10)。

【0 0 1 0】

$$B_{k,j} = h^{k-i_j-1} (g^{x_j} (I V_j))$$

その応答情報  $B_{k,j}$  を送受信部 2 7 から開票装置 1 2 へ送信し、次の  $k$  の問合せを待つ (S 11)。

開票装置 1 2 は図 5 に示すように送受信部 3 1 に応答情報  $B_{k,j}$  が受信されると (S 5)、 $B_{k,j}$  を  $h$  演算部 3 4 に入力して  $B_{k,j}$  に対し一方向性関数  $h$  を施す (S 6)。この演算結果  $h (B_{k,j})$  と記憶部 3 3 内の  $j$  に対する登録情報  $A_j$  と等しいかを調べ (S 7)、 $h (B_{k,j}) = A_j$  であればその受信した  $B_{k,j}$  を  $A_j$  として記憶部 3 3 に記憶して  $A_j$  を更新する (S 8)。全参加者装置からの応答情報に対して、同様の処理を行い、全参加者装置からの応答情報に対する処理が終れば (S 9)、カウンタ 1 3 の値  $k$  を 1 減算して (S 10)、その  $k$  について登録したかの問合せを各参加者装置に対して行う。

【0 0 1 1】

参加者装置 1 1<sub>j</sub> において、 $k$  の問合せが、自分の意中のものであれば、つまり記憶部 2 4 内の  $i_j$  と等しければ (S 9)、図 3 に示すように  $I V_j$  と  $x_j - 1$  を  $g$  演算部 2 5 に入力して  $I V_j$  に対し一方向性関数  $g$  を  $x_j - 1$  回施して応答情報  $B_{k,j} = g^{x_j-1} (I V_j)$  を求め (S 12)、その  $B_{k,j}$  を開票装置 1 2 へ送信

する (S 1 3)。

応答情報  $B_{k,j}$  が意中の指標値と等しいことを示す  $g^{xj-1}(IV_j)$  の場合は、開票装置 1 2 におけるステップ S 7 (図 5) で  $h(B_{k,j})$  が  $A_j = h^{ij+1-ij-1}(g^{xj}(IV_j)) = g^{xj}(IV_j)$  と等しくならない。そこで  $B_{k,j}$  を  $g$  演算部 3 5 に入力して、 $B_{k,j}$  に対し一方向性関数  $g$  を施し、 $g(B_{k,j})$  を求め (S 1 1)、 $g(B_{k,j})$  と記憶部 3 3 内の  $j$  に対する  $A_j$  と等しいかを調べる (S 1 2)。参加者装置 1 1  $j$  が正しい処理をしていたならば、前回の  $k = i_j + 1$  に対する問合せ時に、ステップ S 8 の処理により  $h^{ij+1-ij-1}(g^{xj}(IV_j)) = g^{xj}(IV_j) = A_j$  となっているから、 $g(B_{k,j}) = A_j$  が成立する。この  $k$  を順次減少させる問合せ処理において、最初に  $g(B_{k,j}) = A_j$  が成立した  $k$  が全参加者の意中の指標値中で最大の値であり、この  $k$  を換算テーブル 2 1 を参照して値  $P_k$  に変換し (S 1 3)、その値  $P_k$  を登録した値中の最大値として出力し、必要に応じてその参加者  $j$  も出力する (S 1 4)。

#### 【0 0 1 2】

参加者装置 1 1  $j$  では  $k$  登録かの問合せを受けた時に、 $k = i_j$  であれば (図 3 ステップ S 9)、ステップ S 1 3 で  $B_{k,j}$  と共に問合せのあった  $k$  と自己の意中の  $i_j$  とが等しいことを示す情報 (同一を示す情報) も開票装置 1 2 へ送信するようにしてもよい。この場合は開票装置 1 2 では図 5 中のステップ S 5 で  $B_{k,j}$  を受信すると、同一を示す情報を受信したかを調べ、同一を示す情報を受信していなければ  $h(B_{k,j})$  の演算を行い、同一を示す情報を受信していれば  $g(B_{k,j})$  の演算を行う。なお図 5 中のステップ S 1 2 で  $g(B_{k,j}) = A_j$  とならなければ不正があったとして処理を中止して全員に再登録をさせるとか、あるいはその参加者装置に対する問合せを中止し、他の参加者装置に対する問合せを継続させるようにするなどが考えられる。

#### 【0 0 1 3】

また換算テーブル 2 1 として図 6 に示すように、 $N$  種の指標値 1, 2, 3, ...,  $N$  に対し、値  $P_k$  をその大きい値に 3 0 0 0, 2 9 1 3, 2 9 0 0, ..., 1 0 0 のように対応付けたものを用いれば、 $k$  の問合せで最初に  $g(B_{k,j}) = A_j$  となった  $k$  と対応する  $P_k$  は全参加者の意中の値中の最小値を求めたことになる。

場合によっては換算テーブル 2 1 を使用することなく、指標値の最大値を求めるようにしてもよい。この場合は参加者装置で指標値  $i_j$  を入力し、図 5 中のステップ S 1 2 の次に、指標値  $k$  を最大値として出力し、必要に応じてその参加者  $j$  も出力する。

【0 0 1 4】

参加者装置 1 1  $j$ 、中央装置 1 2 はそれぞれ、コンピュータにより機能させることもできる。

【0 0 1 5】

【発明の効果】

従来の方法ではその値の正当性を検証するために、1 指標値、1 参加者ごとに

$$h(B_{k,j}) = A_j$$

$$g(B_{k,j}) = C_j$$

が成立するか 2 つの検証が必要であったが、この発明ではその値の正当性を検証するために、1 指標値、1 参加者ごとに

$$h(B_{k,j}) = A_j$$

または

$$g(B_{k,j}) = A_j$$

のいずれか一方が成立するか 1 つの検証だけで済み、従来法と比べ、最大値選定または最小値選定を選定されないものの値を明かさないという特徴を保ちつつ処理量を半減できる。

【図面の簡単な説明】

【図 1】

この発明の実施例のシステム構成を示す図。

【図 2】

図 1 中の参加者装置 1 1  $j$  の機能構成例を示す図。

【図 3】

参加者装置 1 1  $j$  における処理手順の例を示す流れ図。

【図 4】

図 1 中の中央装置 1 2 の機能構成例を示す図。

【図 5】

中央装置 1 2 における処理手順の例を示す流れ図。

【図 6】

換算テーブルの他の例を示す図。

【図 7】

従来の電子入札システムを示す図。

【書類名】

図面

【図 1】

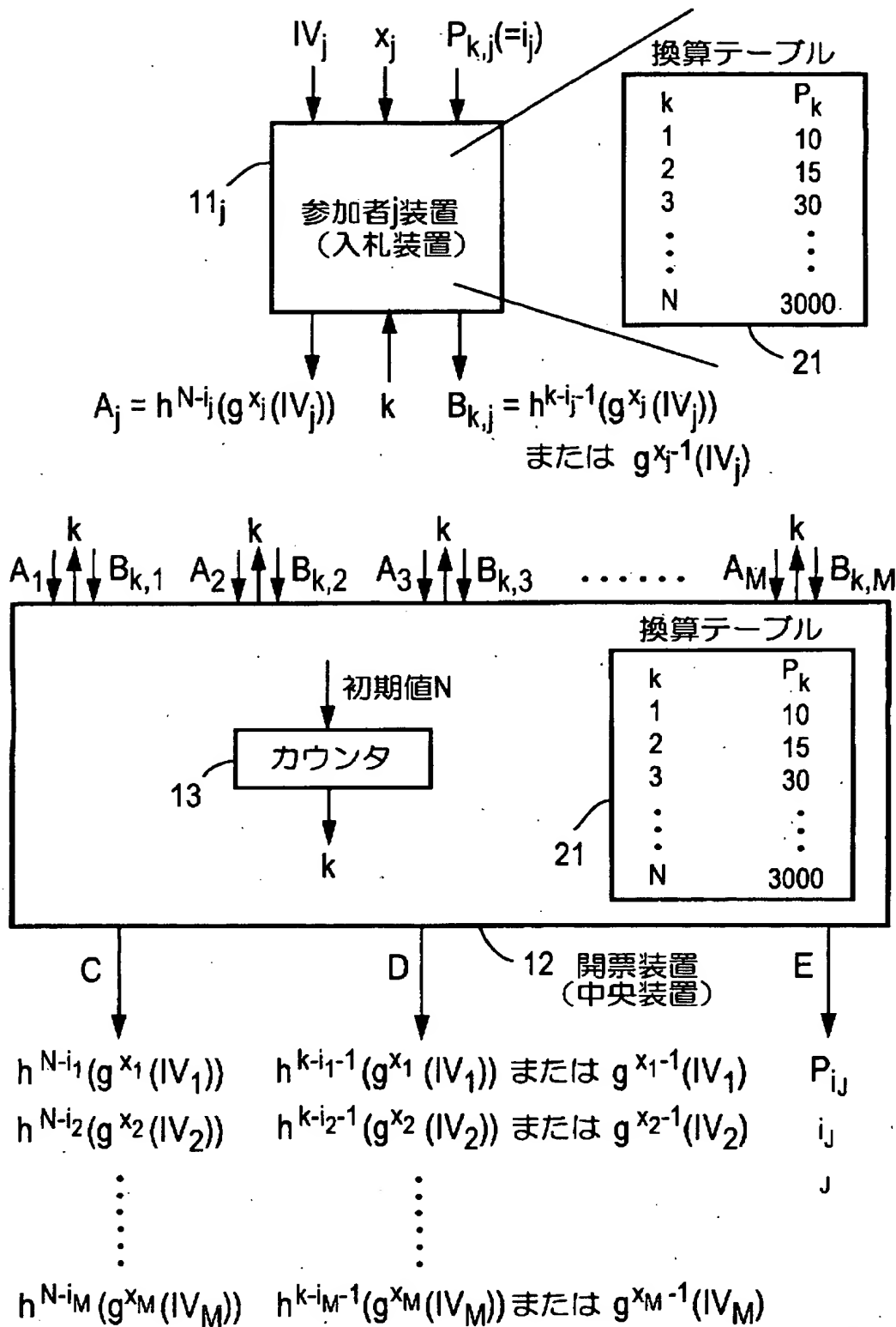


図1

【図 2】

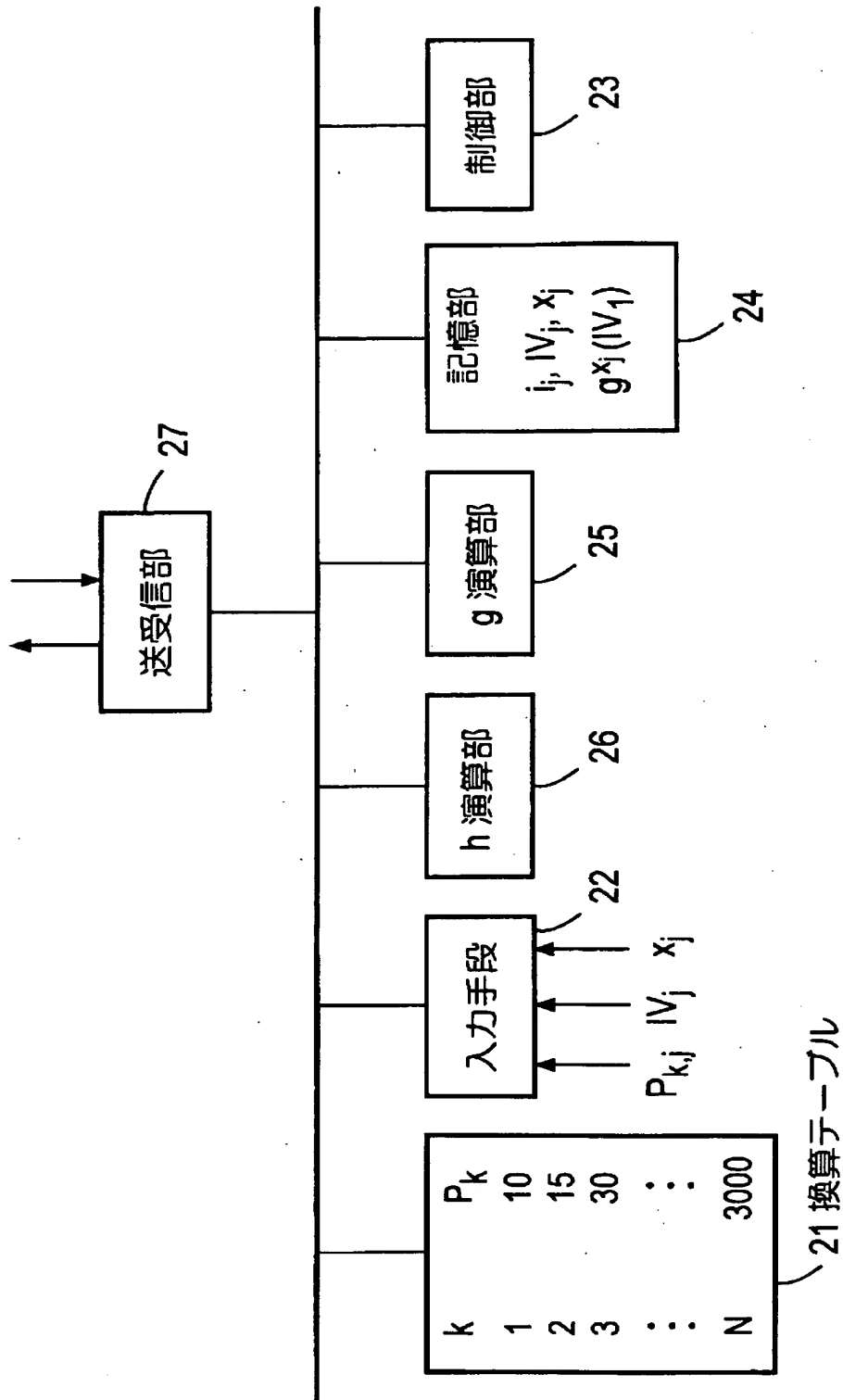


図2



【図 3】

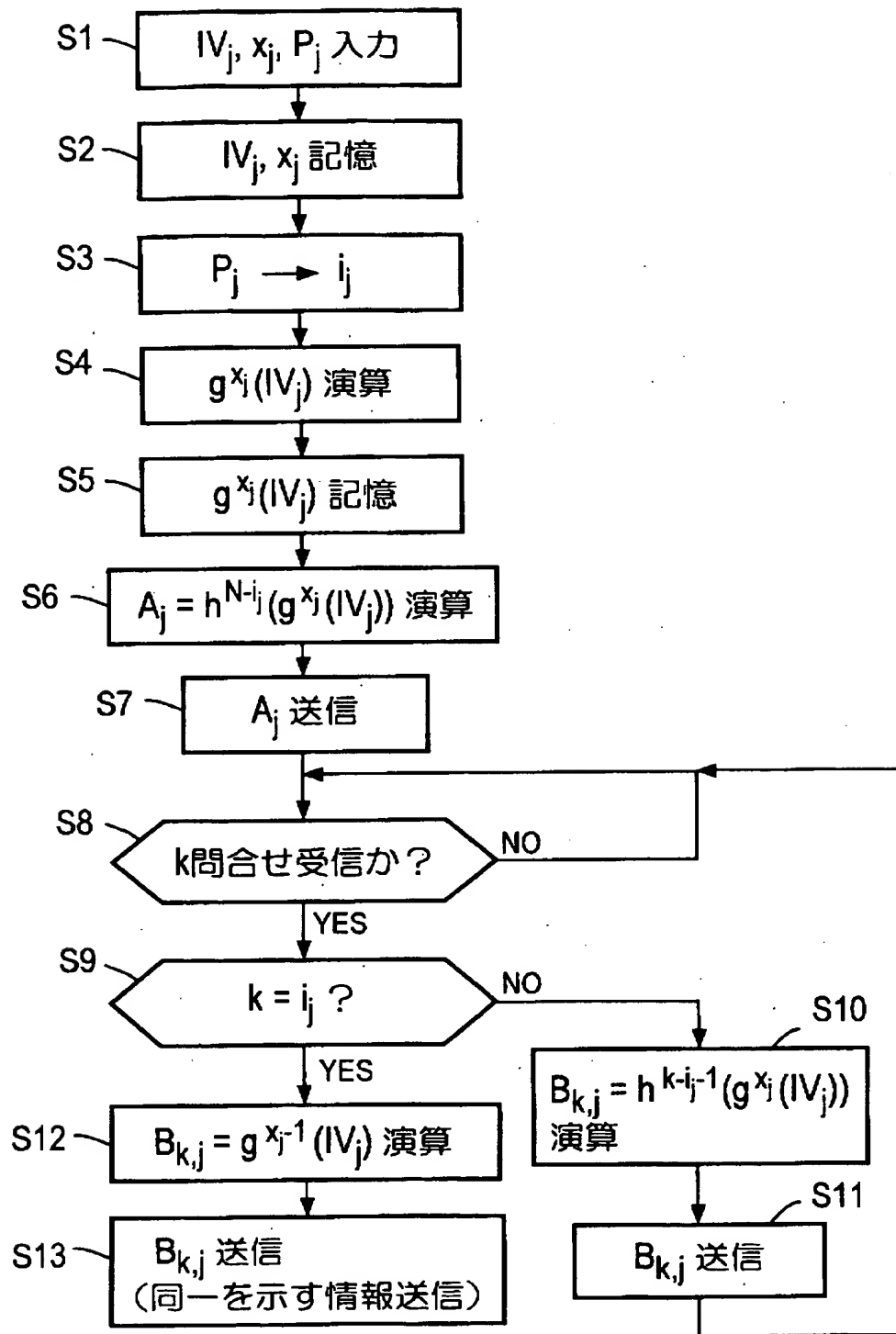


図3

【図 4】

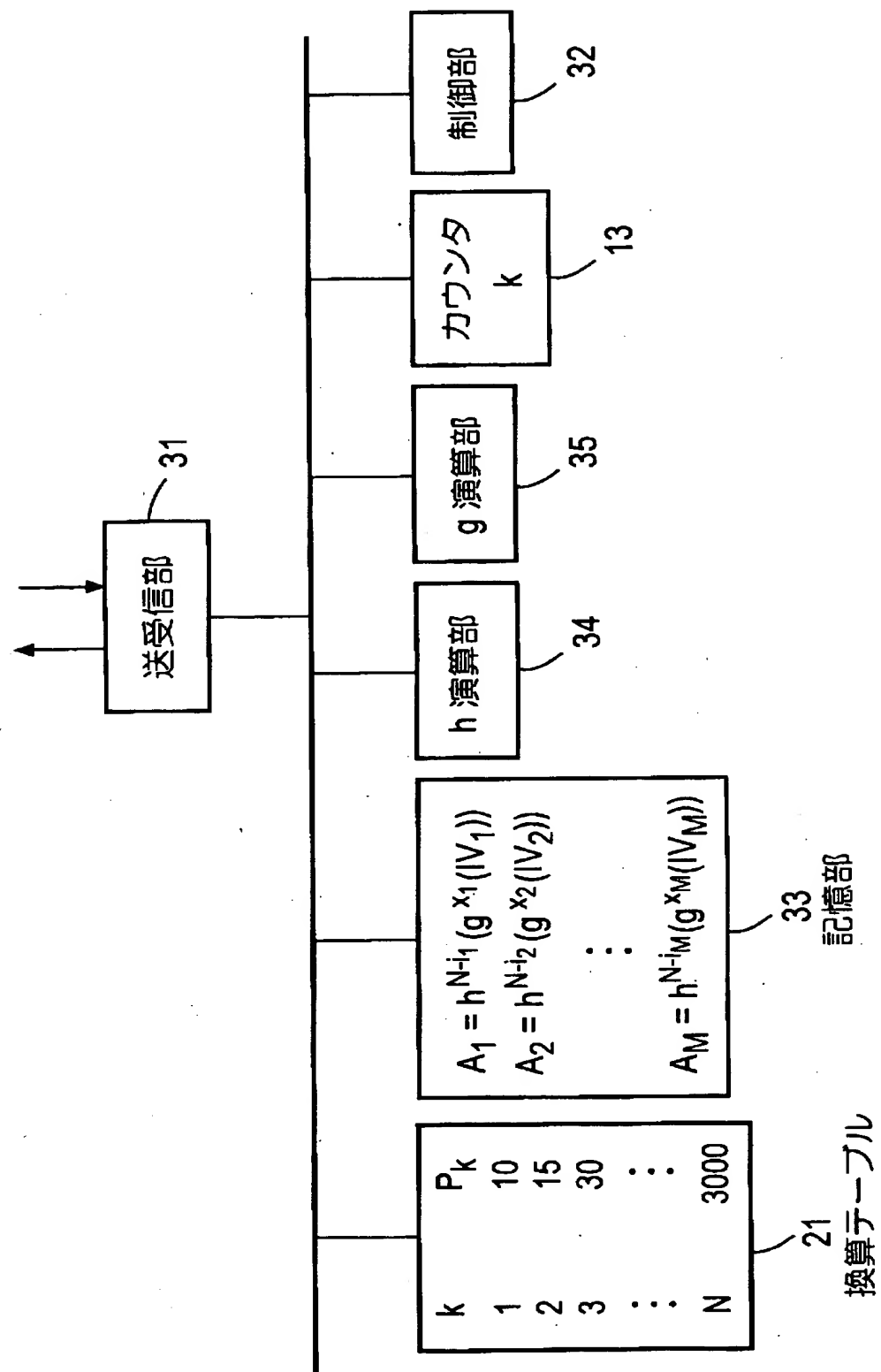


図4

【図 5】

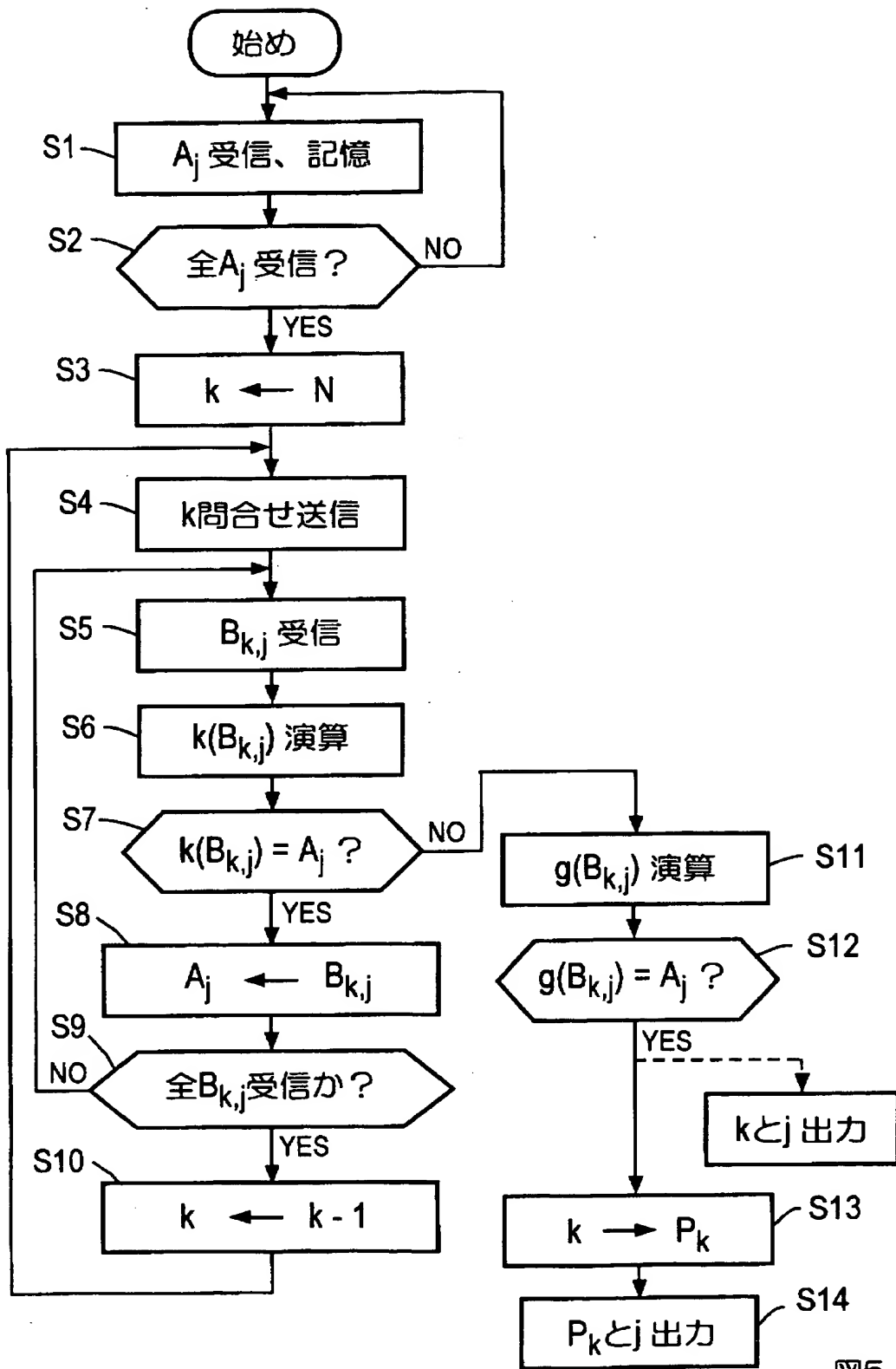


図5

【図 6】

換算テーブル

$k$	$P_k$
1	3000
2	2913
3	2900
$\vdots$	$\vdots$
$N$	100

21

図6

【図 7】

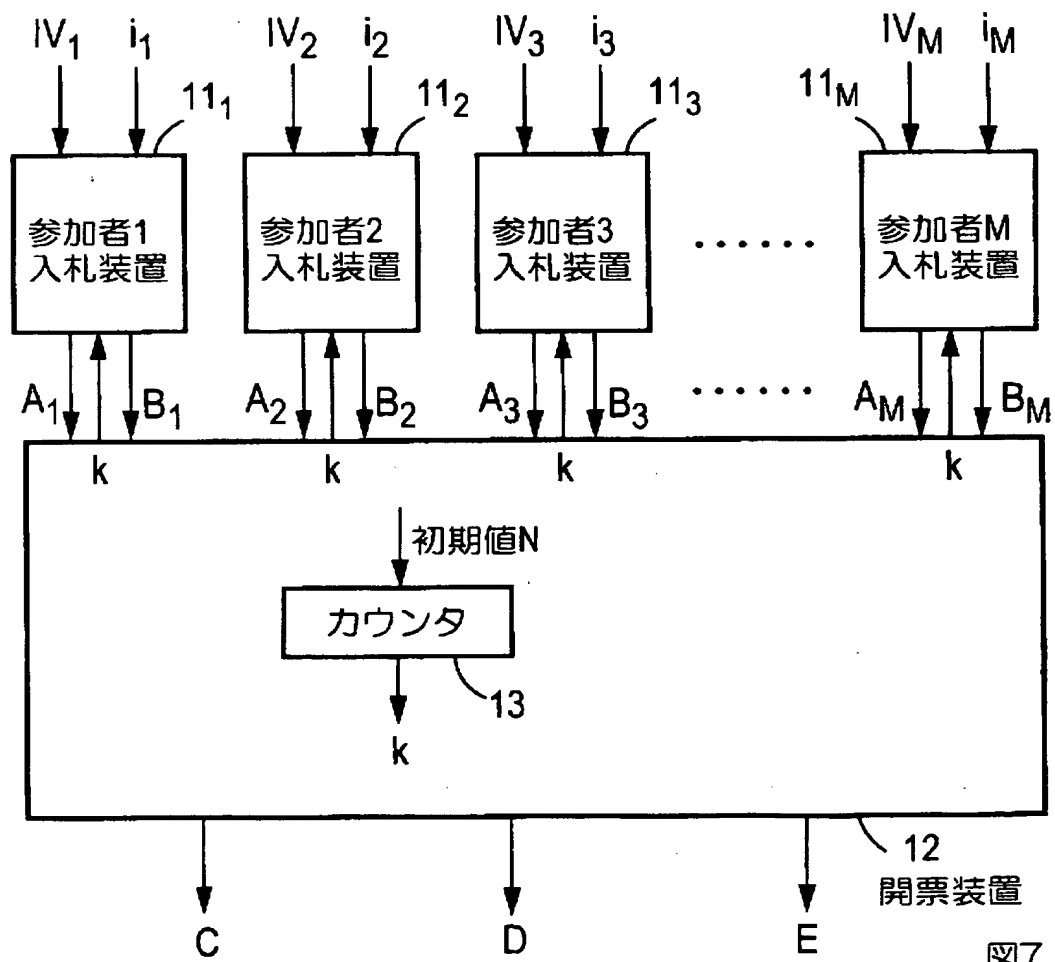


図7

【書類名】 要約書

【要約】

【課題】 検証演算量を減少させる。

【解決手段】 各参加者  $j$  は  $N$  種の指標値  $1, 2, \dots, N$  から選んだ 1 つ  $i_j$ 、初期値  $IV_j$ 、1 以上の任意整数  $x_j$  を入力し、 $IV_j$  に対し一方向性関数を  $x_j$  回施して  $g^{x_j}(IV_j)$  を求め、更に一方向性関数  $h$  を  $N - i_j$  回施して  $A_j = h^{N-i_j}(g^{x_j}(IV_j))$  を開票装置 12 へ送って  $i_j$  を登録し、装置 12 は全参加者からの  $A_j$  を受信後、 $k = N, N-1, \dots, 1$  と順次、 $k$  で登録したかを尋ね、参加者は  $k$  と異なる値を登録した場合は  $B_{k,j} = h^{k-i_j-1}(g^{x_j}(IV_j))$  を、装置 12 へ送り装置 12 は  $h(B_{k,j}) = A_j$  であることを確認して、 $A_j$  の値を  $B_{k,j}$  に変更し、 $k$  を登録した場合は参加者は  $B_{k,j} = g^{x_j-1}(IV_j)$  を装置 12 へ送り、装置 12 は  $g(B_{k,j}) = A_j$  を確認して、その  $k$  を登録した指標値の最大値とする。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000004226]

1. 変更年月日	1999年 7月15日
[変更理由]	住所変更
住 所	東京都千代田区大手町二丁目3番1号
氏 名	日本電信電話株式会社